UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/031,834	06/07/2002	Stanley T. Chow	GSH 08-885347	5762

7590 01/04/2006

Norman P Soloway
Hayes Soloway
130 W Cushing Street
Tucson, AZ 85701

EXAMINER	
MIZAN, SHAHIN	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 01/04/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/031,834	CHOW ET AL.	
	Examiner	Art Unit	
	Shahin Mizan	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 June 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 June 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *6/19/02*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-27 have been examined.

Priority

2. Applicant is advised that as far as the priority claims in the application, neither of the two claims has been properly made in this national stage application. There is a declaration that claims priority to a US provisional and a regular US application. However, the means by which applicant attempted to claim priority is not proper. MPEP 201.11, Section III, indicates the requirement that the application contain a reference to the prior application, which should appear as the first sentence of the specification and/or on the application data sheet - reference in the declaration is not sufficient for claims under 35 USC 120 or 119(e). Since the international application has a filing date prior to the effective date of the American Invention Protection Act, November 29, 2000, the claim to priority can be added at any time before the patent issues. However, at this point, there is no priority claim. As for the claim under 35 USC 120 non-provisional application 09/329,117, it also does not comply with the provisions of 35 USC 120 and 37 CFR 1.78(2)(i) which require that the specific reference to the earlier filed application include the relationship between the PCT and the earlier application.

Specification

3. The disclosure is objected to because of the following informalities:

a. Page 10/ line 3: "data flies" should be changed to "data files"

Appropriate corrections are required.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1 and 20 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 1 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Applicant claims a code obscurifying method in claim 1. This process might be performed without the aid of any technology and therefore the claimed method is not within the technological ads.

All that is necessary to make a sequence of operational steps in a statutory process within 35 U.S.C. 101 is that it be in the technological arts so as to be in concordance with the Constitutional purpose to promote the progress of "useful arts" *In re Musgrave*, 431 F.2d 882 167 USPQ 280 (CCPA 1970).

A claim is limited to a practical application when the method, as claimed, produces a concrete, tangible and useful result: i.e. the method recites a step or act of producing something that is concrete, tangible and useful. *See AT&T v. Excel Communications Inc.*, 172 F.3d at 1358, 50 USPQ2d 1452.

Claim 20 makes use of signals embodied in a carrier wave and is therefore not statutory because it is not tangibly embodied.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Collberg et al. (US Patent 6,668,325).

As per independent claim 1, Collberg et al. teaches a method of increasing the obscurity and tamper-resistance of a software program, comprising the steps of:

randomly generating substantive yet redundant arguments *(note column 37, lines 13-29 - randomness transformation is described; also note algorithm 3 in column 34; also note column 37, lines 64-67 – additional obfuscation techniques are useable as well; also note Fig. 2e and Fig. 2f)*; and

inserting said arguments into the data flow of said program *(note column 37, lines 13-29 - randomness transformation is described; also note algorithm 3 in column 34; also note section 6.2.1 in column 16 – the idea of insertion is defined; also note section 6.2.6; also note Fig. 5, 6, & 31)*.

As per claim 2, which is dependent on claim 1, Collberg et al. teaches a method as claimed in claim 1, wherein said steps of randomly generating and inserting comprise the steps of:

randomly generating substantive yet redundant, lookup tables *(note Fig. 6; also note column 37, lines 13-29 - randomness transformation is described; also note algorithm 3 in column 34; also note claim 76; also note column 23)*; and

inserting said lookup tables into the data flow of said program *(note Fig. 6; also note column 37, lines 13-29 - randomness transformation is described; also note algorithm 3 in column 34; also note Fig. 2c-2g)*.

As per claim 3, which is dependent on claim 2, Collberg et al. teaches a method as claimed in claim 2, wherein said steps of randomly generating and inserting comprise the steps of:

introducing longitudinal diffusion by:

randomly generating identity look up tables *(note column 37, lines 13-29 - randomness transformation is described; also note algorithm 3 in column 34; also note Fig. 2c-2g)*; and

inserting said identity look up tables into the data flow of said program *(note column 37, lines 13-29 - randomness transformation is described; also note algorithm 3 in column 34; also note Fig. 2c-2g)*.

As per claim 4, which is dependent on claim 3, Collberg et al. teaches a method as claimed in claim 3, wherein said program is a data encryption standard (DES) program and said step of randomly generating comprises the step of randomly generating DES-based identities as networks of T-boxes *(note column 38, lines 5-10 - the invention is applicable to DES and other program; also note column 37, lines 13-29 - randomness transformation is described; also note algorithm 3 in column 34; also note Fig. 2c-2g)*.

As per claim 5, which is dependent on claim 4, Collberg et al. teaches a method as claimed in claim 4, wherein said DES-based identities comprise complementary encryption and decryption lookup tables containing a cryptographic key unlike the secret cryptographic key of said DES program *(note column 38, lines 5-10 - the invention is applicable to DES and other programs; also note column 37, lines 13-29 - randomness transformation is described;*

also note algorithm 3 in column 34; also note Fig. 2c-2g).

As per claim 6, which is dependent on claim 5, Collberg et al. teaches a method as claimed in claim 5, wherein said step of inserting comprises the step of:

placing said DES-based identities before and after one or more initial round pairs of said DES program, and before and after one or more final round pairs, thereby defending against attacks from the ends of said DES program *(note column 38, lines 5-10 - the invention is applicable to DES and other program; also note column 37, lines 13-29 - randomness transformation is described; also note algorithm 3 in column 34; also note Fig. 2c-2g).*

As per claim 7, which is dependent on claim 2, Collberg et al. teaches a method as claimed in claim 2, wherein said steps of randomly generating and inserting comprise the steps of:

splitting the data flow of said program into separate streams *(note column 37, lines 13-29 - randomness transformation is described; also note algorithm 3 in column 34; also note Fig. 2c-2g; also note Fig. 29 & 31 and associated description in the specification)*; and

diffusing data laterally between said separate streams *(note columns 31-36 - the algorithms describe the stated function; also note column 37, lines 13-29 - randomness transformation is described; also note algorithm 3 in column 34; also note Fig. 2c-2g; also note Fig. 29 & 31).*

As per claim 8, which is dependent on claim 2, Collberg et al. teaches a method as claimed in claim 2, wherein said steps of randomly generating and inserting comprise the steps of:

introducing lateral diffusion by:

generating multiple lookup tables for an original lookup table *(note Fig. 6; also note claim 76; also note column 23; also note columns 31-36 - the algorithms describes the*

stated function; also note column 37, lines 13-29 - randomness transformation is described; also note algorithm 3 in column 34; also note Fig. 2c-2g; also note Fig. 29 & 31);

generating entries for said multiple lookup tables in accordance with a random Boolean function *(note Fig. 6; also note claim 76; also note column 23; also note columns 31-36 - the algorithms describes the stated function; also note column 37, lines 13-29 - randomness transformation is described; also note algorithm 3 in column 34; also note Fig. 2c-2g; also note Fig. 29 & 31)*; and

transposing the output of said multiple lookup tables in accordance with said random Boolean function *(note Fig. 6; also note claim 76; also note column 23; also note columns 31-36 - the algorithms describes the stated function; also note column 37, lines 13-29 - randomness transformation is described; also note algorithm 3 in column 34; also note Fig. 2c-2g; also note Fig. 29 & 31)*.

As per claim 9, which is dependent on claim 8, Collberg et al. teaches a method as claimed in claim 8, wherein said step of generating entries comprises:

choosing a random, substantive, Boolean function *(note Fig. 5 & 6; also note claim 76; also note sections 6 & 7 in the specification; also note column 37, lines 13-29 - randomness transformation is described; also note algorithm 3 in column 34; also note Fig. 2c-2g; also note Fig. 29 & 31)*;

for each output of said original lookup table:

determining the set of inputs to said Boolean function that will yield said output of said original lookup table *(note Fig. 5 & 6; also note claim 76; also note sections 6 & 7 in the specification; also note column 37, lines 13-29 - randomness transformation is described; also note algorithm 3 in column 34; also note Fig. 2c-2g; also note Fig. 29 & 31)*;

randomly selecting one of said sets of inputs *(also note column 37, lines 13-29 -*

randomness transformation is described; also note algorithm 3 in column 34; also note Fig. 2c-2g; also note Fig. 29 & 31); and

inserting said selected set of inputs, into the output of said multiple lookup tables *(note Fig. 5 & 6; also note claim 76; also note sections 6 & 7 in the specification; also note column 37, lines 13-29 - randomness transformation is described; also note algorithm 3 in column 34; also note Fig. 2c-2g; also note Fig. 29 & 31)*;

modifying calls to said original lookup table to call upon said multiple lookup tables *(note Fig. 5 & 6; also note claim 76; also note sections 6 & 7 in the specification; also note column 37, lines 13-29 - randomness transformation is described; also note algorithm 3 in column 34; also note Fig. 2c-2g; also note Fig. 29 & 31)*; and

inserting said random Boolean function into the data flow of said program following said calls to said multiple lookup tables *(note Fig. 5 & 6; also note claim 76; also note sections 6 & 7 in the specification; also note column 37, lines 13-29 - randomness transformation is described; also note algorithm 3 in column 34; also note Fig. 2c-2g; also note Fig. 29 & 31)*.

As per claim 10, which is dependent on claim 9, Collberg et al. teaches a method as claimed in claim 9, wherein said random Boolean function is a two input Boolean function and each said set of inputs comprises two inputs *(note Fig. 5 & 6; also note claim 71 & 76; also note sections 6 & 7 in the specification; also note column 37, lines 13-29 - randomness transformation is described; also note algorithm 3 in column 34; also note Fig. 2c-2g; also note Fig. 29 & 31)*.

As per claim 11, which is dependent on claim 9, Collberg et al. teaches a method as claimed in claim 9, wherein said random Boolean function is a three input Boolean function and each said set of inputs comprises three inputs *(note Fig. 5 & 6; also note claim 71 & 76; also note sections 6 & 7 in the specification; also note column 37, lines 13-29 - randomness*

transformation is described; also note algorithm 3 in column 34; also note Fig. 2c-2g; also note Fig. 29 & 31).

As per claim 12, which is dependent on claim 10, Collberg et al. teaches a method as claimed in either of claims 10, wherein said steps are executed beginning at penultimate lookup tables, and working backwards towards earlier rounds*(note Fig. 5 & 6; also note claim 71 & 76; also note sections 6 & 7 in the specification; also note column 37, lines 13-29 - randomness transformation is described; also note algorithm 3 in column 34; also note Fig. 2c-2g; also note Fig. 29 & 31).*

As per claim 13, which is dependent on claim 6, Collberg et al. teaches a method as claimed in either of claims 6, wherein said software program is an encryption program requiring a cryptographic key, said method comprising the previous step of:

converting said software program into a direct acyclic graph *(note sections 3, 4, 5 - the techniques for performing the stated function is described; also note Fig. 5 & 6; also note claims 71 & 76; also note sections 6 & 7 in the specification; also note Fig. 2c-2g; also note Fig. 29 & 31).*

As per claim 14, which is dependent on claim 13, Collberg et al. teaches a method as claimed in claim 13, wherein said encryption program is a Data Encryption Standard (DES) program and said step of converting comprises the steps of:

unrolling the n digital encryption software algorithm rounds by:

duplicating the round network n times and connecting said n rounds end-to-end *(note column 37, lines 64-67 - the invention is applicable to DES; also note column 38, lines 5-9; also note sections 3, 4, 5 - the techniques for performing the stated function is described; also note Fig. 5 & 6; also note claims 71 & 76; also note sections 6 & 7 in the specification; also note Fig. 2c-2g; also note Fig. 29 & 31)*;

copying the i S-boxes explicitly into each round, resulting in n x i separate S-boxes *(note column 37, lines 64-67 - the invention is applicable to DES; also note column 38, lines 5-9; also note sections 3, 4, 5 - the techniques for performing the stated function is described; also note Fig. 5 & 6; also note claim 71 & 76; also note sections 6 & 7 in the specification; also note Fig. 2c-2g; also note Fig. 29 & 31)*; and

converting each said k-output S-box into k 1-output T-boxes resulting in n x i x k separate T-boxes, with k x i separate T-boxes per round *(note column 37, lines 64-67 - the invention is applicable to DES; also note column 38, lines 5-9; also note sections 3, 4, 5 - the techniques for performing the stated function is described; also note Fig. 5 & 6; also note claim 71 & 76; also note sections 6 & 7 in the specification; also note Fig. 2c-2g; also note Fig. 29 & 31).*

As per claim 15, which is dependent on claim 14, Collberg et al. teaches a method as claimed in claim 13, wherein said step of converting comprises the step of:

unrolling the sixteen digital encryption software algorithm rounds by:

duplicating the round network sixteen times and connecting said rounds end-to end *(note column 37, lines 64-67 - the invention is applicable to DES; also note column 38, lines 5-9; also note sections 3, 4, 5 - the techniques for performing the stated function is described; also note Fig. 5 & 6; also note claim 71 & 76; also note sections 6 & 7 in the specification; also note Fig. 2c-2g; also note Fig. 29 & 31)*;

copying the eight S-boxes explicitly into each round, resulting in 128 separate S-boxes *(note column 37, lines 64-67 - the invention is applicable to DES; also note column 38, lines 5-9; also note sections 3, 4, 5 - the techniques for performing the stated function is described; also note Fig. 5 & 6; also note claim 71 & 76; also note sections 6 & 7 in the specification; also note Fig. 2c-2g; also note Fig. 29 & 31)*; and

converting each said 4-output S-box into four 1-output T-boxes resulting in 512

separate T-boxes, thirty-two per round *(note column 37, lines 64-67 - the invention is applicable to DES; also note column 38, lines 5-9; also note sections 3, 4, 5 - the techniques for performing the stated function is described; also note Fig. 5 & 6; also note claim 71 & 76; also note sections 6 & 7 in the specification; also note Fig. 2c-2g; also note Fig. 29 & 31)*.

As per claim 16, which is dependent on claim 15, Collberg et al. teaches a method as claimed in claim 15, further comprising the step of:

partially evaluating said program to eliminate the cryptographic key as a separate constant or series of constants *(note column 37, lines 64-67 - the invention is applicable to DES; also note column 38, lines 5-9; also note sections 3, 4, 5 - the techniques for performing the stated function is described; also note Fig. 5 & 6)*.

As per claim 17, which is dependent on claim 16, Collberg et al. teaches a method as claimed in claim 16. further comprising the step of:

where one operand of an XOR operation adjacent to a T-box is a constant, eliminating said XOR operation by:

modifying the entries of said T-box to effect said XOR accordingly *(note column 37, lines 64-67 - the invention is applicable to DES; also note column 38, lines 5-9; also note sections 3, 4, 5 - the techniques for performing the stated function is described; also note Fig. 5 & 6)*; and

deleting said XOR operation *(note column 37, lines 64-67 - the invention is applicable to DES; also note column 38, lines 5-9; also note sections 3, 4, 5 - the techniques for performing the stated function is described; also note Fig. 5 & 6)*.

As per independent claim 18, Collberg et al. teaches an apparatus for increasing the obscurity and tamper-resistance of computer software code comprising:

means for modifying said software code by:

randomly generating substantive yet redundant arguments *(note column 37, lines 13-29 - randomness transformation is described; also note algorithm 3 in column 34; also note column 37, lines 64-67 – additional obfuscation techniques are useable as well; also note Fig. 2e and Fig. 2f)*; and

inserting said arguments into the data flow of said software code *(note column 37, lines 13-29 - randomness transformation is described; also note algorithm 3 in column 34; also note section 6.2.1 in column 16 – the idea of insertion is defined; also note section 6.2.6; also note Fig. 5, 6, & 31)*.

As per claim 19, Collberg et al. teaches a computer readable memory medium, storing computer software code executable to perform the steps of claim 1 *(note Fig. 1 and exemplary hardware in column 4 – describes the hardware and software required to perform the functions of the invention)*.

As per claim 20, Collberg et al. teaches a computer data signal embodied in a carrier wave, said computer data signal comprising a set of machine executable code being executable by a computer to perform the steps of claim 1 *(note Fig. 1 and exemplary hardware in column 4 – describes the hardware and software required to perform the functions of the invention; also note the LAN in 1st paragraph that could have wireless means of communication or one of the I/O port can be configured for wireless communication)*.

As per claim 21, which is dependent on claim 1, Collberg et al. teaches the method as claimed in claim 1, wherein said substantive yet redundant arguments are substantive in that said arguments are applied to variables used in said software program, and that said arguments alter the value of said variables *(note Fig. 1 and exemplary hardware in column 4; also note sections 4-6 in the specification)*.

As per claim 22, which is dependent on claim 11, Collberg et al. teaches a

method as claimed in claim 11, wherein said steps are executed beginning at penultimate lookup tables, and working backwards towards earlier rounds *(note Fig. 1 and exemplary hardware in column 4; also note sections 4-6 in the specification)*.

As per claim 23, which is dependent on claim 12, Collberg et al. teaches a method as claimed in claim 12, wherein said software program is an encryption program requiring a cryptographic key, said method comprising the previous step of:

converting said software program into a direct acyclic graph *(note Fig. 1 and exemplary hardware in column 4; also note sections 4-6 in the specification; also note Fig. 5 & 6)*.

As per claim 24, which is dependent on claim 23, Collberg et al. teaches a method as claimed in claim 23, wherein said encryption program is a Data Encryption Standard (DES) program and said step of converting comprises the steps of:

unrolling the n digital encryption software algorithm rounds by:

duplicating the round network n times and connecting said n rounds end-to-end *(note column 37, lines 64-67 - the invention is applicable to DES; also note column 38, lines 5-9; also note sections 3, 4, 5 - the techniques for performing the stated function is described; also note Fig. 5 & 6; also note claim 71 & 76; also note sections 6 & 7 in the specification; also note Fig. 2c-2g; also note Fig. 29 & 31)*;

copying the i S-boxes explicitly into each round, resulting in n x i separate S-boxes *(note column 37, lines 64-67 - the invention is applicable to DES; also note column 38, lines 5-9; also note sections 3, 4, 5 - the techniques for performing the stated function is described; also note Fig. 5 & 6; also note claim 71 & 76; also note sections 6 & 7 in the specification; also note Fig. 2c-2g; also note Fig. 29 & 31)*; and

converting each said k-output S-box into k 1-output T-boxes resulting in n x i x k

separate T-boxes, with k x i separate T-boxes per round *(note column 37, lines 64-67 - the invention is applicable to DES; also note column 38, lines 5-9; also note sections 3, 4, 5 - the techniques for performing the stated function is described; also note Fig. 5 & 6; also note claim 71 & 76; also note sections 6 & 7 in the specification; also note Fig. 2c-2g; also note Fig. 29 & 31)*.

As per claim 25, which is dependent on claim 24, Collberg et al. teaches a method as claimed in claim 24, wherein said step of converting comprises the step of:

unrolling the sixteen digital encryption software algorithm rounds by:

duplicating the round network sixteen times and connecting said rounds end-to end *(note column 37, lines 64-67 - the invention is applicable to DES; also note column 38, lines 5-9; also note sections 3, 4, 5 - the techniques for performing the stated function is described; also note Fig. 5 & 6; also note claim 71 & 76; also note sections 6 & 7 in the specification; also note Fig. 2c-2g; also note Fig. 29 & 31)*;

copying the eight S-boxes explicitly into each round, resulting in 128 separate S-boxes *(note column 37, lines 64-67 - the invention is applicable to DES; also note column 38, lines 5-9; also note sections 3, 4, 5 - the techniques for performing the stated function is described; also note Fig. 5 & 6; also note claim 71 & 76; also note sections 6 & 7 in the specification; also note Fig. 2c-2g; also note Fig. 29 & 31)*; and

converting each said 4-output S-box into four 1-output T-boxes resulting in 512 separate T-boxes, thirty-two per round *(note column 37, lines 64-67 - the invention is applicable to DES; also note column 38, lines 5-9; also note sections 3, 4, 5 - the techniques for performing the stated function is described; also note Fig. 5 & 6; also note claim 71 & 76; also note sections 6 & 7 in the specification; also note Fig. 2c-2g; also note Fig. 29 & 31)*.

As per claim 26, which is dependent on claim 25, Collberg et al. teaches a method as claimed in claim 25, further comprising the step of:

partially evaluating said program to eliminate the cryptographic key as a separate constant or series of constants *(note column 37, lines 64-67 - the invention is applicable to DES; also note column 38, lines 5-9; also note sections 3, 4, 5 - the techniques for performing the stated function is described; also note Fig. 5 & 6)*.

As per claim 27, which is dependent on claim 26, Collberg et al. teaches a method as claimed in claim 26, further comprising the step of:

where one operand of an XOR operation adjacent to a T-box is a constant, eliminating said XOR operation by:

modifying the entries of said T-box to effect said XOR accordingly *(note column 37, lines 64-67 - the invention is applicable to DES; also note column 38, lines 5-9; also note sections 3, 4, 5 - the techniques for performing the stated function is described; also note Fig. 5 & 6)*; and

deleting said XOR operation *(note column 37, lines 64-67 - the invention is applicable to DES; also note column 38, lines 5-9; also note sections 3, 4, 5 - the techniques for performing the stated function is described; also note Fig. 5 & 6)*.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Johnson et al. (US Patent No. 6,088,452) teaches an encoding technique for software and hardware.

Nardone et al. (US Patent No. 6,205,550) teaches tamper resistant methods and apparatus.

Sander et al. "Towards Mobile Cryptography", International Computer Science

Institute, TR-97-049, Nov. 22, 1997.

http://citeseer.ist.psu.edu/cache/papers/cs/3445/ftp:zSzzSzftp.icsi.berkeley.eduzSzpubzSztechreportszSz1997zSztr-97-049.pdf/towards-mobile-cryptography.pdf

Sander et al. "Protecting Mobile Agents Against Malicious Hosts", G. Vigna (ed), Mobile Agent Security, Feb., 1998.

http://www.cs.virginia.edu/~jones/cs551S/papers/protect_mobile_agent_against_host.pdf#search='Protecting%20Mobile%20Agents%20Against%20Malicious%20Hosts'

Inquiries

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shahin Mizan whose telephone number is 571-272-0687 and whose fax number is 571-273-0687. The examiner can normally be reached on M-F 8:30 a.m. - 5:00 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

	Shahin Mizan Examiner Art Unit 2132

SM

THOMAS R. PEESO
PRIMARY EXAMINER